16th ICCRTS

"Collective C2 in Multinational Civil-Military Operations"

Towards Building Trusted Multinational Civil-Military Relationships Using Social Networks

Paper number: 114

Topic 4: Information and Knowledge Exploitation

Bruce Forrester
Defence R&D Canada – Valcartier
2459 Pie-XI North
Quebec, QC, G3J 1X5
Tel.: (418) 844-4000 #4943
Bruce.Forrester@drdc-rddc.gc.ca

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Towards Building Trusted Multinational Civil-Military Relationships Using Social Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defence R&D Canada - Valcartier,2459 Pie-XI North,Quebec, QC, G3J 1X5,**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

Presented at the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011), Qu?c City, Qu?c, Canada, June 21-23, 2011. U.S. Government or Federal Rights License.

14. ABSTRACT

Trust in relationships is essential for deep sharing of information/intelligence and meaningful collaboration. Building the required level of trust is often a lengthy face-to-face process. Lack of trust seriously hampers effectiveness in situations such as emergency response to international crisis or the coming together of a coalition. Specifically, it leads to redundant analysis and information overload. Trust-based networks are a very promising avenue. Trust can be mapped to the digital world, at least partially, through attributes associated with Social Networking technologies. When combined with recommendation systems, trust-based results are better than traditional collaborative filtering techniques [1]. These systems have proven effective in finding good films to watch or for feeling confident about online purchasing, but can they be adapted to more high-stake endeavours such as intelligence information gathering? Since 2005, we have witnesses an unprecedented technological adaption rate in the form of social networking applications and the use of such recommender systems. However use by military and Other Government Departments (OGDs) has been very conservative. Can the formation of a military, OGD and Non-Government Organizations (NGO) social network allow for meaningful information sharing and trust between multinational civil-military actors? Would such a network increase access to pertinent operational information while decreasing the information overload of intelligence analysts? This paper takes a first look at the concepts of, trust, social networking, recommender systems and how they could be combined to decrease information overload.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**33**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Towards Building Trusted Multinational Civil-Military Relationships Using Social Networks

Bruce Forrester
Defence R&D Canada – Valcartier
Bruce.Forrester@drdc-rddc.gc.ca

Abstract

Trust in relationships is essential for deep sharing of information/intelligence and meaningful collaboration. Building the required level of trust is often a lengthy face-to-face process. Lack of trust seriously hampers effectiveness in situations such as emergency response to international crisis or the coming together of a coalition. Specifically, it leads to redundant analysis and information overload. Trust-based networks are a very promising avenue. Trust can be mapped to the digital world, at least partially, through attributes associated with Social Networking technologies. When combined with recommendation systems, trust-based results are better than traditional collaborative filtering techniques [1]. These systems have proven effective in finding good films to watch or for feeling confident about online purchasing, but can they be adapted to more high-stake endeavours such as intelligence information gathering? Since 2005, we have witnesses an unprecedented technological adaption rate in the form of social networking applications and the use of such recommender systems. However use by military and Other Government Departments (OGDs) has been very conservative. Can the formation of a military, OGD and Non-Government Organizations (NGO) social network allow for meaningful information sharing and trust between multinational civil-military actors? Would such a network increase access to pertinent operational information while decreasing the information overload of intelligence analysts? This paper takes a first look at the concepts of, trust, social networking, recommender systems and how they could be combined to decrease information overload.

To begin with, we have to avoid confusion between familiarity and trust. Familiarity is an unavoidable fact of life; trust is a solution for specific problems of risk. But trust has to be achieved within a familiar world, and changes may occur in the familiar features of the world which will have an impact on the possibility of developing trust in human relations. Hence we cannot neglect the conditions of familiarity and its limits when we set out to explore the conditions of trust [2].

I Introduction

In an increasingly complex and rapidly changing operational environment, commanders, decision makers, and personnel rely on accurate, timely, and relevant information that can be stored and maintained securely and accessed quickly at headquarters and in the field. In today's world, and in the future, our ability to exploit (find, manipulate, combine, purposely use and share) the huge stores of data and information will be a key contributor to success.

However, the sheer volume of information produced, and the increasing number of available channels for its creation and communication, challenge our capabilities to fully understand, leverage and effectively manage and share information assets. At the same time, complex national

security issues such as asymmetric cyber and bio-terrorism, environmental degradation, and ethnic unrest, religious extremism and resource disputes require that military operations are conducted at an accelerated pace, requiring rapid coordination of political and military objectives and increasing dependence upon information and intelligence. The information sharing requirement is no less applicable between militaries, governments and Non-Government Organizations (NGOs) in time of crisis as has been witnessed with such events as the Hurricane Katrina, Asian Tsunamis, and the Haïtian Earthquake. Such complexity has spawned many initiatives to improve the flow of information such as the NATO Core Enterprise Services Framework [3], the United Kingdom Warfighter Information Services Framework [4-6], and the Canadian Future Intelligence Analysis Capability . However, overwhelmingly these initiatives rely on the machines and algorithms to sort through the mass quantities of information and do not specifically include the power of social networks and the concept of the long tail[7] to attack the problem of information overload.

Research has shown that "a distributed knowledge system serves to reduce individual cognitive overload, enlarge the collective pool of expertise, and minimize redundancy" [8]. A large number of web-based tools could be used to provide a platform for such a pool of expertise. This platform could take the form of a social network. The development of social networks has been an inherent part of human society since the dawn of Man, however, the growth of the Internet over the past 20 years has given rise to an era of human interconnection like no other.

This paper is investigative in nature and as such will start with a scenario to set the stage for possible research into a social network that allows for the building of trust between members. The aim of such a network would be to encourage the type of deep sharing of information between disparate organizations, who perhaps have the tendency to distrust one another, which is required for successful resolution of international crisis events. Next the paper examines some of the domains important to building such a social network. It concludes with the viability of such a network and poses important research questions that would need to be answered before such a network could be built.

II Scenario

Major Jones was part of the first rotation into the Haïti, just two months after the fast-reaction teams were sent in. As an Intelligence officer, he knew the importance of building good relationships. Relationships built trust and trust leads to a good flow of information and intelligence. Apart from leaving his family for six months, he was actually looking forward to this deployment. During his pre-deployment training, he had participated in a new initiative that was focused on building trust between intelligence analysts, and the various military and the non-government organizations that had flocked to the disaster zone to help the Haitian people.

This new initiative was quite a different approach to this problem than his last deployment, in the southern Afghan theatre, when such a program was not yet in place. He distinctly remembered the time that fellow soldiers were killed in an operation to rescue a reporter who had gotten himself into trouble; despite having been warned not to travel into that particular area, the reporter ignored the advice and was taken by Taliban[9]. After that, it was hard to convince his troops to show patience with the NGOs. However, he believed that this time, the military could concentrate on achieving their missions without having to worry about the safety of NGOs. Indeed, the NGOs would be aiding his own task as they report on activities and participate in a network that enables information sharing and relationship building.

The introductions and information sharing had stared soon after the quake in Haïti about two months ago. Shortly after he received his travel orders he was advised to log into the METIS network (named after the Titan Goddess of good counsel, advice, planning and wisdom). METIS was set up to allow individuals from government departments and from non-government organizations, as well as contractors from industry, to interact prior to and during deployment to countries in need of aid. The idea was to build relationships through online social networking that would then translate into trust, or at least better understanding of one another, on the ground in the theatre of operations. In fact, Major Jones remembered that he met some of his most important contacts in the communal coffee garden area in Afghanistan [9].

Over the next two months, he read through the homepage of each of the NGO's that provided its missions and objectives and profiled its people. He read the profiles, blogs and comments from many individuals who were already working Haïti, as well as many more who were scheduled to go. He found that some had very similar interests and he was able to trade some tips on finer points of home brewing. He was able to ask questions and determine some additional kit that he would need. Perhaps most important, he was able to discuss his mission and help sort out how the many organizations on the ground could better work together to help the Haïtian people. "But as the past few months have made clear, there is little coordination among the NGOs or between the NGOs and Haitian officials. Some NGO plans don't fit or clash outright with the plans of the government. Some are geared toward short-term relief—a classic case of giving a man a fish instead of teaching him to fish"[10]. Jones was hoping that METIS would aid in changing this problem.

Another aspect of METIS was the ability to upload materials relevant to the operation. Maj Jones was feeling overwhelmed with the amount of information and reports that he needed to read in order to get up to speed on Haïti. Luckily, the METIS had a trust-based recommendation system that allowed him to quickly hone in on the most pertinent documents as well as the experts in various areas.

Now in theatre, Maj Jones was using the METIS system daily to get updates on NGO movements. As well, he was able to see what other analysts were reading and recommending. This included all sorts of OSINT (open source intelligence) and HUMINT (human intelligence) sources as well as NGO situation reports.

III Information and Intelligence

From a Canadian perspective, an intelligence capacity is essential to all military operations and permeates throughout the hierarchal levels from the strategic down to the tactical. Its function is to support commanders and their staffs in decision making through timely and accurate understanding of the adversary and operational environment. During operations, an intelligence analyst must aid in the commander's understanding of the plethora of characteristics pertaining to the enemy, security, and conditions in the operational environment [11]. Whether during kinetic operations or in response to a crisis, there is a never ending stream of information arriving at the Intelligence Analyst's computer. "No operation can be planned with real hope of success until sufficient information on the adversary and environment has been obtained and converted into intelligence" [12]. We must be aware of the distinction between information and intelligence as shown in figure 1.

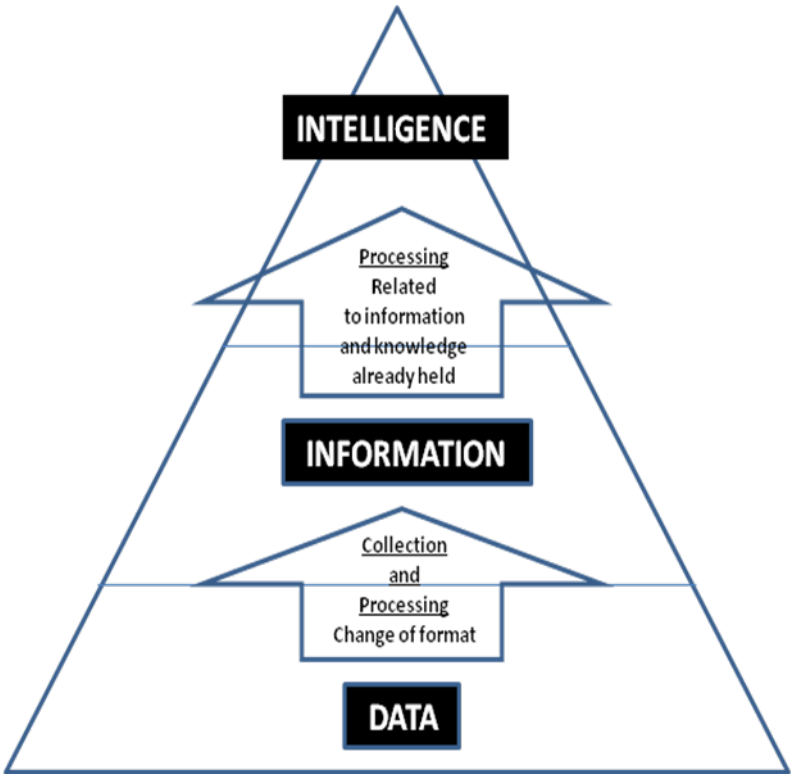


Figure 1 Information and Intelligence Relationship

Information consists of data captured by sensors (electronic or human) that presents a statement of what exists or has existed at a specific place and time. NATO defines information as "unprocessed data of every description which may be used in the production of intelligence"[13]. Intelligence is defined as "the product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements or areas of actual or potential operations." [13]. The term is also applied to the activity which gives rise to intelligence and as a generic title, to those who carry out the process, which leads to its production. Information is turned into intelligence that supports the various situational awareness pictures (Blue – own forces; Red – adversary forces; Green – neutral; Brown – environmental)[14].

A very important source for basic and current intelligence comes from Open Source Intelligence (OSINT). It is intentionally discovered and discriminated unclassified information that can be used to address questions. Because of its freely available nature, it can alleviate the need for classified intelligence information collection resources [15]. This is the type of information that will most likely be exchanged in a trust-based recommendation system.

IV Information Overload

Let's define one of the problems that already effects 21st century militaries. There are mountains of information and knowledge available to anyone connected to the Internet. Compare this incredible access to 1993, less than two decades ago. At that time, one needed access to a library or an expert to get in-depth information. A common problem now is information overload – the difficulty a person can have understanding an issue and making decisions that can be caused by the presence of too much information [16]. In addition to the ever increasing time needed to search through the

information, there is an increased likelihood that relevant information will be overlooked. However, this is by no means a new phenomenon. Blair [17] describes strategies used by early scholars reacting to the overabundance of books as early as the 1550s. In 2006, the amount of digital information created, captured, and replicated was 1,288 x 1018 bits. In computer parlance, that's 161 exabytes or 161 billion gigabytes … This is about 3 million times the information in all the books ever written [18].

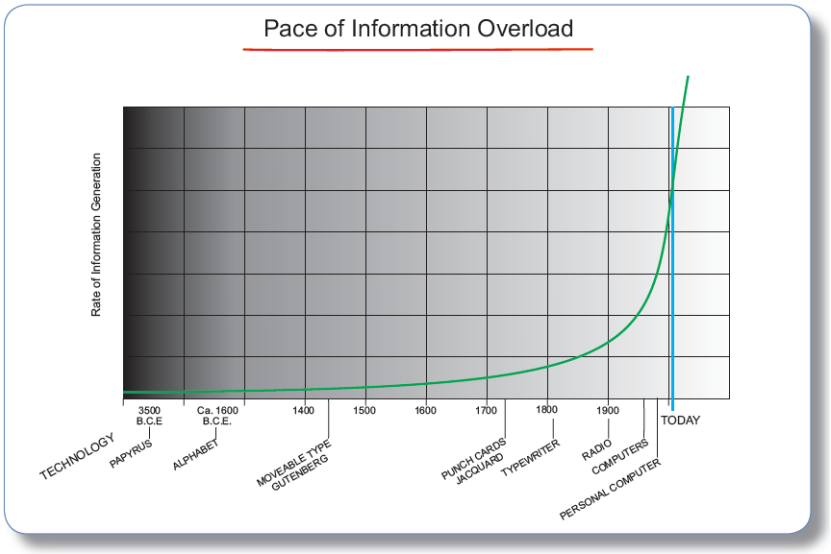


Figure 2 Facilitative technology versus rate of information generation

As shown in figure 2, the availability of technology to the masses has played an important role in the generation of information. Between 2006 and 2010, the information added annually to the digital universe increased more than six fold from 161 exabytes to 988 exabytes [18]. If you are not already, you will soon be overwhelmed.

V Trust Research

Trust has been studied by psychologists as an individual conceptualization along personality theory [19, 20] and from a behavioural perspective in the classic prisoner's dilemma game [21]. While a great deal of research has been conducted in these areas, no general theme or consistent definition of trust has emerged and this has led to much confusion [22]. These social scientists focused on uncovering the psychological states of people as individuals. However, neither of these lines of research adequately explains the social nature of trust. Trust is complex and multidimensional. It appears cognitively, behaviourally, affectively and is dependent on the context (situation), but these traits do not necessarily manifest together. Hence trying to isolate individual components through reductionist methodology simplifies the study of trust to the point of missing its true nature. Lewis implores us to think of trust as a property of collective units [22].

From a sociological perspective, trust is studied through the relationships between people rather than the individual psychological states of people. Trust permeates through members of a group or society when they are confident that others will act in an expected manner. For example, Sue will

share a secret with Barb because she trusts her not to spread the secret, however she no longer trusts Gail, who gossiped Sue's last secret. Trust in organizations and institutions leads to a stable society. We collectively show trust in our money and financial institutions by our investments and unquestioning use of our currency. When this trust no longer exists, counties quickly become unstable. It is this sociological view of trust that is most applicable and useful in the case of taking advantage of the power of social networks. However, trust must be operationalized.

The definition of trust adopted by Golbeck is simple and can be easily modeled in a computational system: "trust in a person is a commitment to an action based on a belief that the future actions of that person will lead to a good outcome"[1]. Luhmann states, "Trust is only required if a bad outcome would make you regret your action" [2]. He argues that the function of trust is "the reduction of complexity" [22]. This latter statement is valuable in understanding how trust plays a role in the reduction of information overload through the employment of trust based systems combined with social networks. Both trust and distrust will tend to decrease complexity; however trust can form the basis to decrease an individual's (intelligence analysts) workload with respect to information while distrust will increase this load through an increased suspicion and the requirement to monitor, verify and recheck. Of interest in this potential research is how the trust built in social networks has been exploited to produce recommendations. There are several recent studies that have looked at automated agents. Walter et al [23] use the following definition of trust for their model, "the expectancy of an agent to be able to rely on some other agent's recommendations" (p.2).

Lewis identifies three distinct dimensions of trust: cognitive, emotional, and behavioural that are merged into a unitary social experience [22]. The cognitive aspect allows one to explain their evidence for trusting a person or institution. It is what we know about a person; the evidence or reasons to trust that person. However, such knowledge only sets up a platform from which to make the cognitive leap beyond the rational reasons. We are able to make this "trust leap" because collectively we all need to make this leap and "trust in trust" [24]. However this alone is not enough. The emotional dimension of trust must compliment this cognitive base. We have all felt the immense pain when the emotional aspect of trust has been betrayed by a friend, family member, or lover. Likewise on a societal level we feel the outrage when a representative of an important institution betrays our trust (the church, clergy, police, military). The third component is the behavioural enactment of trust. Lewis states, "behaviourally, to trust is to act as if the uncertain future actions of others were indeed certain in circumstances wherein the violation of these expectations results in negative consequences for those involved" [22]. It is this behavioural aspect that helps to create a platform based on the reciprocal nature of trust; we tend to trust those who trust us [24].

The notion of trust inherent in social networks has been modeled in several research initiatives [1, 23, 25-28]. However, the models and algorithms used to date remain oversimplified and do not fully represent the complexities of the dynamic nature of a social network nor the concept of trust. For example, most models treat trust as transitive. Calculating the trust between "a" and "d" in Figure 3 would be a matter of summing the trust values of each of the links (a to b, b to c, c to d). However it is not clear that such transitivity exists.

There are other characteristics of trust that also need to be taken into consideration when designing trust algorithms:

a. Trust is dynamic. The degree of trust "b" has in "c" can change over time depending on the interactions and outcomes between the two.

b. Trust is asymmetrical. The degree of trust "b" has for "c" is not necessarily the same that "c" has for "b".
c. Trust has a slow build rate but a quick fall rate.
d. Trust is subjective and personal. "a" and "b" will have different degrees of trust towards "c" and objective measures are very hard to produce.
e. Composability. There are different paths that could be followed to connect "a" and "d" (through b & c or through e, f & c).
f. Trust is context-dependent. "a" might trust "b" to provide information about one country but not about another country.

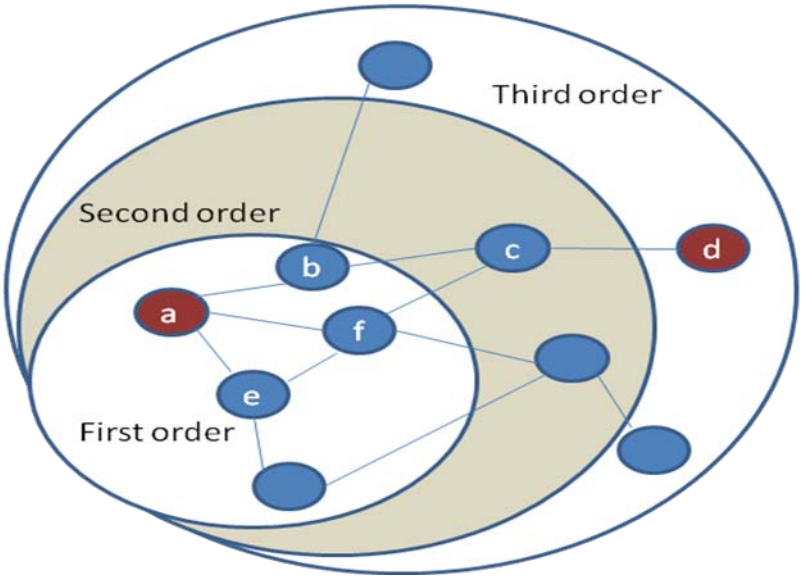


Figure 3 A simple social network and links. First order links are direct neighbours and tend to have high trust between one another. Second order links have less trust because they must pass through first order neighbours. Third order neighbours trust levels are further diminished compared to first order.

VI Recommendation Systems

The use of recommendation systems aids users in rapidly decreasing the size of the pool from which to find objects of interest. It essentially acts as a social filter. The algorithms that sort through user recommendations are usually of two types:

a. those which are based on similarities between the current item of interest and the items related to it (i.e. a site might show you all books that are related to a particular breed of dog), or

b. Those based on the similarities of the users' likes within the system (i.e. Amazon's famous – "users that bought this book also bought these books..."), also known as collaborative filtering.

There are problems with both of these types of filtering. The first (based on similarities) tends to be impersonal as it does not take into consideration the characteristic of the user other than what items they have looked at in the past. In addition, such a system would not be good for finding outliers or emergent items. The second, collaborative filtering requires a database of ratings on the items. This implies that newer items, that are not likely to have many initial ratings, will not be taken in account by the algorithms. In the intelligent analysts' case, the most recent information is critical to the situational awareness and hence collaborative filtering could not be used without significant improvements. The diversity of information will also need to be taken into account. These filtering algorithms tend to recommend only items that are similar. There will need to be a way to get items that are considered outliers or very different for comparison and for hypothesis validation.

Golbeck has taken the collaborative filtering recommendation system further by adding a trust dimension through the combination of a social networking site and a movie rating and review system [1, 26]. Walter et al. [23], use agents at the core of their model and these agents "leverage their social network to *reach information*, and make use of trust relationships to *filter information*" (p.2). Both the models of Golbeck and Walter would require significant improvement to enable use for intelligence gathering purposes. Walter uses a discrete rating (-1 dislike or 1 like) for objects. Golbeck [1] goes further by using a 4-star rating system with the availability of half stars. She concludes that "the accuracy of the trust-based predictive ratings [in the FilmTrust website] is significantly better than the accuracy of a simple average of the ratings assigned to a movie. The trust system also outperforms the recommended ratings from a Person-correlation based recommender system" (p. 102). Such scales would probably not be adequate for the complex nature of information discrimination; experimentation with a user community would be needed to determine a proper scale for information.

Recently, Walter et al. [28] have increased the complexity of their model by accounting for the dynamic nature of trust within a social network. Previous algorithms were not able to account for the fact that the trust one places in another can change depending on the quality of particular recommendations. Trust, in these past models, was assigned a specific static value. In the proposed model by Walter et al. a utility function is added that couples the values of trust with the utility experienced. In empirical testing, they found that their new model had comparable performance to collaborative filtering models. However, it outperformed for recommendations of items that were different from those that a user had already rated. This is an interesting characteristic and could be very useful for intelligence agents that are looking for anomalies or emergent events.

In a similar vein, Moghaddan et al.'s [29] model incorporates the effect of feedback by telling the system the actual rating of the object from a user after having received the ratings of other users within the network. This is similar to the utility function described above. This model uses two components for trust: explorability and dependability. Explorability is an impersonal trust that is based on the properties or reliance on a system or institution within which that trustee exists and not on any property or state of the trustee. Dependability is an interpersonal trust that is the trust one user has in another user. Moghaddan et al. used a large dataset (49k users, 139k objects, 664k rating of these objects) to test their model and concluded that FeedbackTrust outperformed existing trust-based recommenders MoleTruas and TidalTrust in terms of mean absolute error (that measures the deviations of predictions from other users to actual ratings of the receiving user). Interesting, this notion of trust in an institution or organization can be exploited by "pre-trusting" people that belong to certain institutions (a university, NATO, etc).

VII Social Networking

The advent of social-based websites such as Facebook, MySpace, and LinkedIn have changed our ability to connect with old relationships and to make new ones. Since these social links are recorded by the databases backing these sites, there is great potential for exploiting the links. These sites allow users to search out or create groups based on virtually any common thread that could tie people together. There are thousands of communities that come together to discuss and share on their passions or to just chat about classmates. Millions use Facebook to keep in touch with geographically distant family and friends. These sites could easily be thought of as expert locators or sources for finding like-minded people, passionate about similar interests. With the users of Facebook surpassing 69 million and rapidly growing, I believe that we have just scratched the surface on potential uses for social networking. In Facebook, new applications and ways of characterizing your friends are produced weekly. The ease of use and platform independent nature of these sites is significant. Half the world - 3 billion people - own a cell phone. Most are, or soon will be, capable of direct connection to social networking sites. "When users find it easy to connect and open up to others, they become increasingly comfortable uploading and sharing self generated content; frequent interaction builds community, trust, and self-policing norms. Social networking will extend our reach and help to build worldwide trust"[30].

"A social network is a social structure made up of individuals (or organizations) called "nodes", which are tied (connected) by one or more specific types of interdependency, such as friendship, kinship, common interest, financial exchange, dislike, sexual relationships, or relationships of beliefs, knowledge or prestige"[31]. In its simplest form, a social network is a map of specified ties, such as friendship, between the nodes being studied. Social network analysis views social relationships in terms of network theory consisting of nodes and ties (also called edges, links, or connections). There can be many kinds of ties between the nodes. Research [32] in a number of academic fields has shown that social networks operate on many levels, from families up to the level of nations, and play a critical role in determining the way problems are solved, organizations are run, and the degree to which individuals succeed in achieving their goals.

Network technologies represent a dramatic disruptive challenge to the traditional hierarchical organizational structures and processes. So much so that traditional hierarchical organizations such as militaries and government departments have been reluctant and slow to adapt. More profoundly, the emergence of a networked society suggests a quantitatively new avenue of human coordination and self-organization. A main feature of Web 2.0, peer-production, is defined as decentralized yet collaborative information gathering and creation that depends on very large aggregations of individuals independently scouring their information environment in search of opportunities to be creative in small or large increments. These individuals are able to self-identify for tasks and perform them for a variety of motivational reasons. The fundamental advantage of commons-based peer-production lies in a better capability to identify and allocate human creativity available to work on information and cultural resources. Hence, there is a direct connection to open source or human information gathering for intelligence situational awareness.

Peer production in a military context is building a common picture (situational awareness); solving problems together (tactics), and maintaining a progressive discourse (continual improvement and sense-making). It is about the community building artefacts that are used by the community and producing meaningful, personalized information that leads to effective operationally focused capabilities. Realistically, there is far too much data, information, and knowledge out in the world for any single person to make sense of it, even in a highly specialized area such as warfare. The "work of the masses – the wisdom of crowds" will be the only way that we can hope to make sense

of it all. Information and sharing of experiences must feed back into many facets of the military organization.

Despite the slow adaption rate, there have been several military virtual social networking initiatives with the goal of timely information exchange and dissemination. The first such site was Company Command. They state: "We are a grass-roots, voluntary forum that is by and for the profession with a specific, laser-beam focus on company-level command. By joining, you are gaining access to an amazing community of professionals who love Soldiers and are committed to building combat-ready teams" [29]. This was followed by Platoon Leader [30] in a similar vain for that position in the hierarchy. These were initiatives that circumvented the usual information vetting organizations. Other such networks, CAVNet and TIGRNet, and the Canadian ORION (a wiki database for information sharing) are used by deployed troops to exchange information quickly and efficiently by cutting out the bureaucracy [31]. However, all of these grass roots information dissemination methods were initially frowned upon by the high ranking but are now tolerated do to their adaption rates by the working ranks.

Dwyer, Hiltz and Passerini [33] have looked at the willingness of members of a social networking site to share personal information and develop new relationships. They used the popular sites Facebook and MySpace. Their results showed that "Facebook members were more trusting of the site and its members, and more willing to include identifying information in their profile. Yet MySpace members were more active in the development of new relationships"[33]. However the forecast type of information shared in the METIS site would be more of an organizational nature than personal. How will this make a difference?

There is a site named NGOPost.org that encourages NGOs or socially concerned individuals to post their stories and ideas that facilitate action. However there is no one site dedicated to increasing awareness and increasing trust and information sharing between Militaries, OGDs and NGOs.

VIII Conclusion and Questions

There is clear evidence that trust-based recommendation algorithms enable users to sort through vast quantities of information to produce good results, thus decreasing the information overload of individual users. However, the current research has concentrated on low-risk subjects such as movies or opinions on consumer goods. In the intelligence domain, information takes many different forms consisting of anything from large academic papers to short situation reports provided by actors on the ground in an operational theatre. There might be very few recommendations attached to these artefacts thus limiting the usefulness of collective filtering. Although, perhaps one recommendation from a highly trusted neighbour would be enough to warrant attention.

While such algorithms might work for some situations, to be useful for intelligence purposes they would also require a content filter. One might foresee the application of pattern-matching technology [34] that forms a conceptual and contextual understanding of all content, independent of language or format. Combined these two forms of filtering would produce a strong starting point for intelligent analysts.

Some of the questions that will need to be examined in this research are:

a. How does one create an online environment that allows for the right mix of these components of trust such that deep sharing of information can occur?

b. Can the use of personal agents help to create automated trust recommendations?
c. How does the reputation of the organization that one represents affect the level of individual trust?
d. How sophisticated do the algorithms need to be in order to produce good results?
e. There are many issues to resolve from a human factors perspective. Would intelligent analysts and NGOs use such a network?

It is believed that trust-based recommendation algorithms are worth further exploration. Further research, taking the particular nature of intelligence gathering into consideration is warranted.

References

1. Golbeck, J., *Generating Predictive Movie Recommendations from Trust in Social Networks*, in *ITrust 2006*, K. Stolen, Editor 2006.
2. Luhmann, N., *Familiarity, Confidence, Trust: Problems and Alternatives*, in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta, Editor 2000, Department of Sociology, University of Oxford,. p. 94-107.
3. NATO, *NATO Interoperability Standards and Profiles V 2.0*, 2008, C3 CCSC NATO Open Systems Working Group.
4. Bray, S., *Warfighter Information Services Framework*, 2010, Defence Science and Technology Laboratory.
5. Bray, S., *Human and Machine Interaction with Knowledge Bases*, in *15th ICCRTS*2010. p. 29.
6. Bray, S., *A framework for Warfighter Inforamtion Services - using the concpet of a Virtual Knowledge Base*, in *15th ICCRTS*2010. p. 20.
7. Anderson, C., *The Long Tail: Why the Future of Business is Selling Less of More*2006, New York: Brockman.
8. Pronovost, S. and G. Lai, *Virtual Social Networking and Interoperability in the Canadian Forces Netcentric Environment*, J. Crébolder, Editor 2009, Defence R&D Canada - Atlantic.
9. Schurman, D., *Telephone conversation*, B. Forrester, Editor 2001: Ottawa.
10. cordoba, J.d., *Aid Spawns Backlash in Haiti*, in *The Wall Street Journal*2010.
11. Army, U.S., *Intelligence Analysis*, A. U.S, Editor 2009: U.S. Army Intelligence Center.
12. DND, *Joint Intelligence Doctrine*, D.o.N. Defence, Editor 2003, J2 Plans Pol.
13. NATO, *Glossary of Terms and Definitions* 2002.
14. DND, *Land Force Information Operations Field Manual Intelligence*, D.o.N. Defence, Editor 2001.
15. Branch, S.I., *NATO Open Source Intelligence Handbook*, 2001: Norfolk.
16. Wikipedia. *Information Overload*. 2011 [cited 2001 28 January 2001].
17. Blair, A., *Reading Strategies for Coping with Information Overload ca. 1550-1700.* Journal of the History of Ideas, 2003. **64**(1): p. 11-28.
18. Preoccupations. *various statistics on information*. 2007; Available from: http://www.preoccupations.org/2007/03/exponential_inf.html.
19. Rotter, J.B., *A New Scale for the Measurement of Interpersonal Trust.* Journal of Personality, 1967. **35**: p. 651-655.
20. Rotter, J.B., *Generalized Expectancies for Interpersonal Trust.* American Psychologist, 1971. **26**: p. 443-452.
21. Deutsch, M., *Trust and Suspicion.* Journal of Conflict Resolution, 1958. **2**: p. 265-279.

22. Lewis, J.D. and A. Weigert, *Trust as a Social Reality.* Social Forces, 1985. **63**(4): p. 967-985.
23. Walter, F., S. Battiston, and F. Schweitzer, *A model of a trust-based recommendation system on a social network.* Autonomous Agents and Multi-Agent Systems, 2008. **16**(1): p. 57-74.
24. Luhmann, N., *Trust and Power*1979, Chichester: Wiley.
25. Golbeck, J., *Combining Provenance with Trust in Social Networks for Semantic Web Content Filtering*, in *Provenance and Annotation of Data*, L. Moreau and I. Foster, Editors. 2006, Springer Berlin / Heidelberg. p. 101-108.
26. Golbeck, J., *Computing and Applying Trust in Web-based Social Networks*, in *Computer Science*2005, Maryland. p. 185.
27. Walter, F., S. Battiston, and F. Schweitzer, *Coping with Information Overload through Trust-Based Networks*, in *Managing Complexity: Insights, Concepts, Applications*, D. Helbing, Editor 2008, Springer Berlin / Heidelberg. p. 273-300.
28. Walter, F.E., S. Battiston, and F. Schweitzer, *Personalised and dynamic trust in social networks*, in *Proceedings of the third ACM conference on Recommender systems*2009, ACM: New York, New York, USA. p. 197-204.
29. Moghaddam, S., et al., *FeedbackTrust: Using Feedback Effects in Trust-based Recommendation Systems*, in *RecSys '09*2009: New York.
30. Shuen, A., *Web 2.0 A strategy guide*2008, Farnham: O'reilly Media Inc.
31. *Social Network*. Wikipedia, 2011.
32. Christakis, N. and J. Fowler, *Connected: The Surprising Power of Our Social Networks and How They Shape Our lives*2009, New York: Little Brown.
33. Dwyer, C., S. Hiltz, and K. Passerini, *Trust and Privacy Concern within social networking sites: A comparision of Facebook and MySpace*, in *Americas Conference on Information Systems (AMCIS)*2007: Keystone, Colorado.
34. Autonomy. *Conceptual Search*. [cited 2011 29 January]; Available from: http://www.autonomy.com/content/Functionality/idol-functionality-conceptual-search/index.en.html.

DEFENCE R&D DÉFENSE

Towards Building Trusted Multinational Civil-Military Relationships Using Social Networks

Bruce Forrester, PhD

22 June 2011

Defence Research and Development Canada
Recherche et développement pour la défense Canada

Canada

Introduction

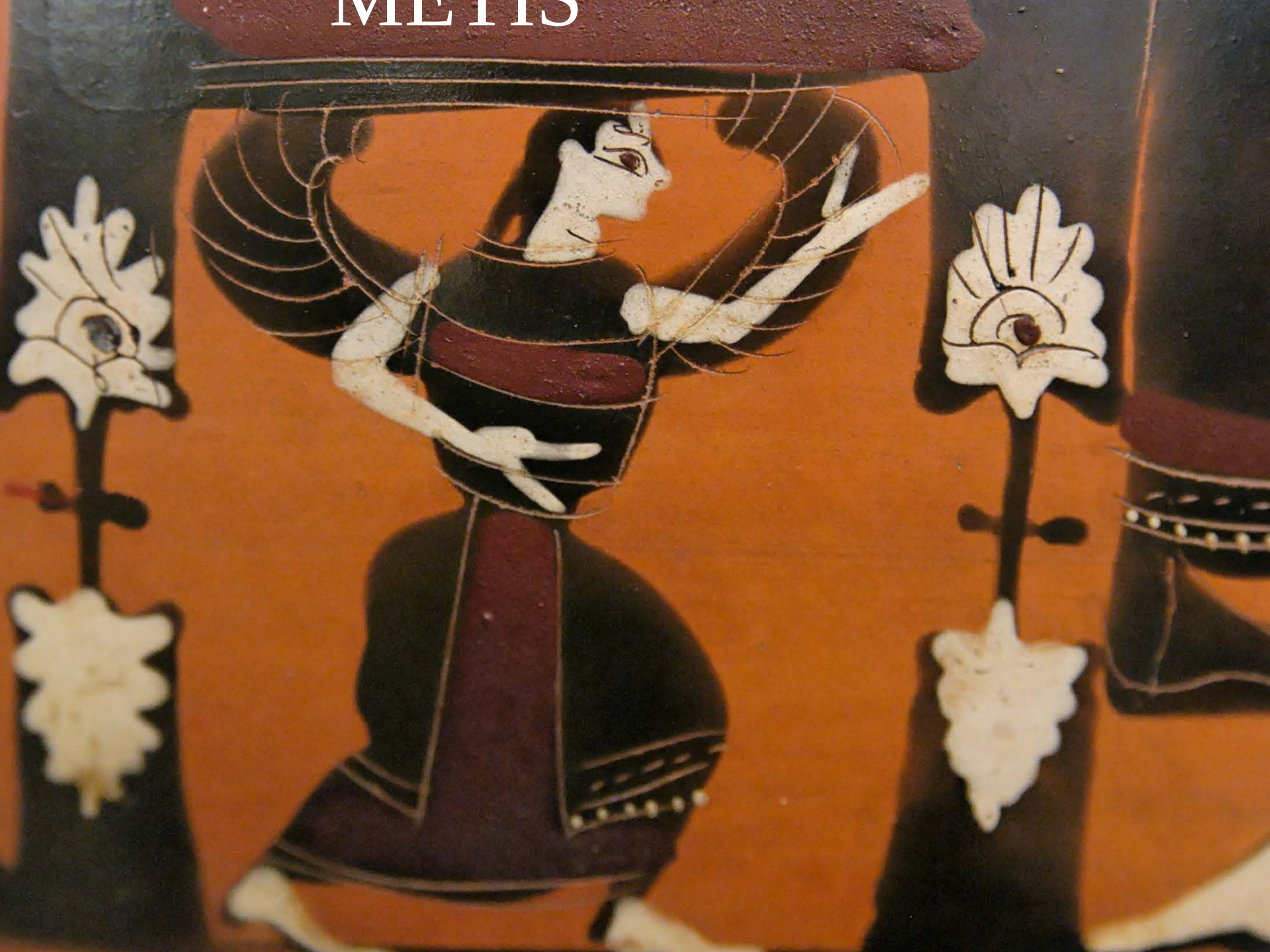
Agenda

- Scenario
- Trust
- Recommendation Systems
- Social Networks
- Challenges
- Conclusion


ISAF


KOREA

METIS




Tim Hortons
WALK IN

MEDECINS SANS FRONTIERES
DOCTORS WITHOUT BORDERS

InterAction
American Council for Voluntary International Action

Save the Children

PARTNERS for DEVELOPMENT

International Medical Corps

NGO non-governmental organization

IFAD
INTERNATIONAL FUND FOR AGRICULTURAL DEVELOPMENT

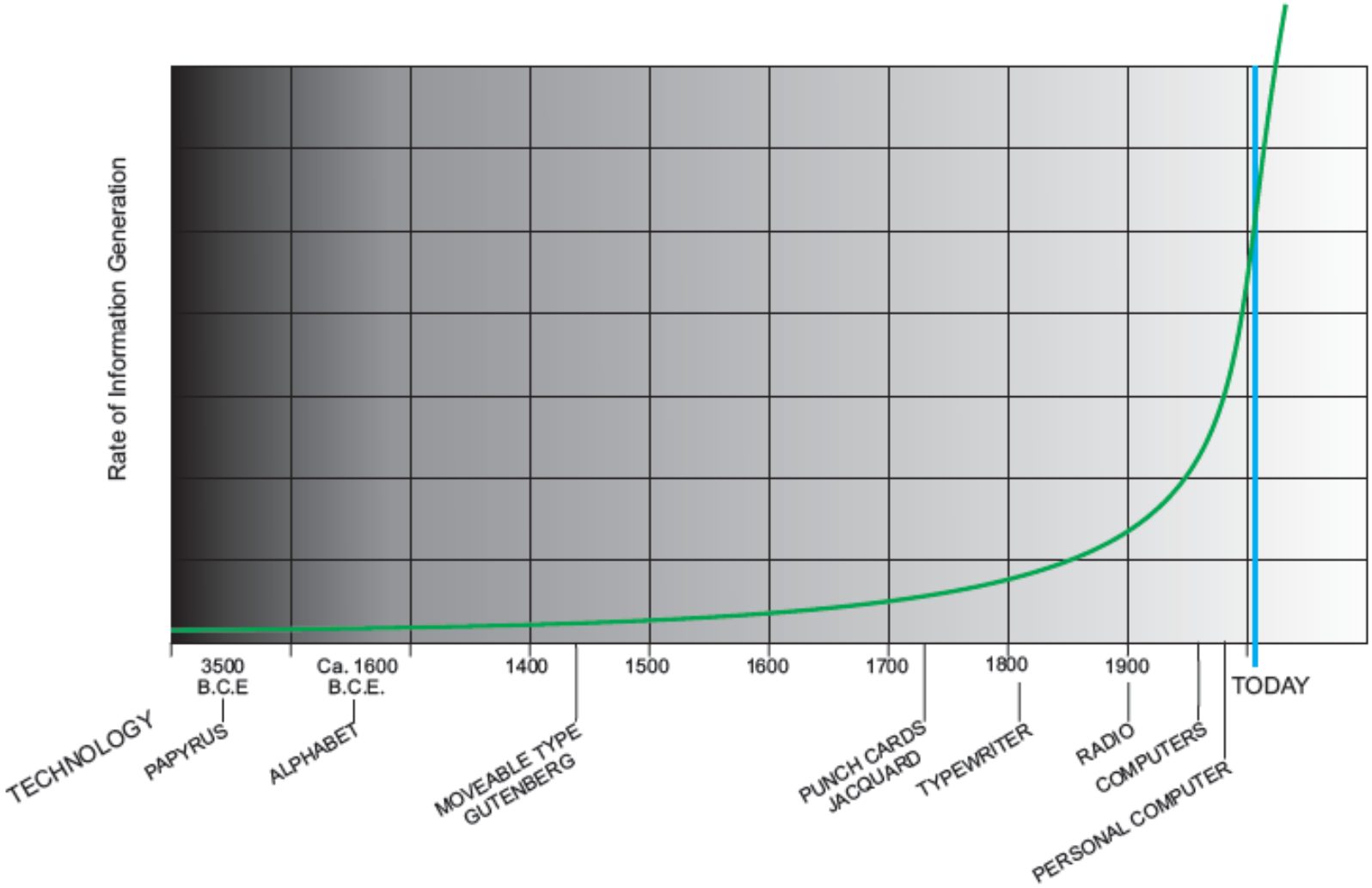
care

World Vision

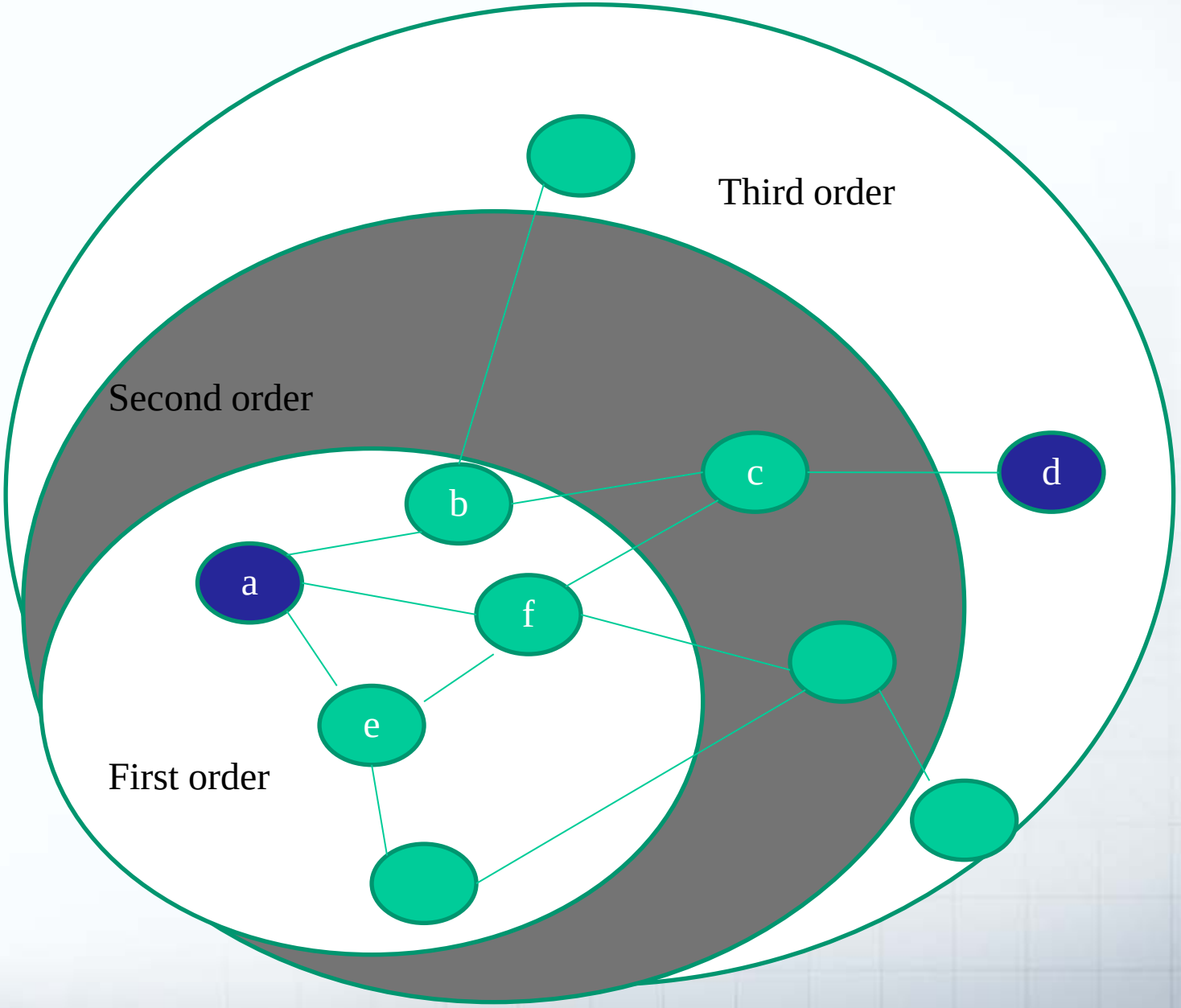
Oxfam International

CRS
CATHOLIC RELIEF SERVICES

Pace of Information Overload



Trust



Recommendation Systems

- Aids users in rapidly decreasing the size of the pool from which to find objects of interest
- Two main types:
  - a site might show you all books that are related to a particular breed of dog
  - Amazon's famous – "users that bought this book also bought these books..."
- Disadvantages
  - Neither are good for emergence
  - Tend to recommend only similar items

Social Networks

Challenges

- How does one create an online environment that allows for the right mix of trust components such that deep sharing of information can occur?
- How does the reputation of the organization that one represents affect the level of individual trust?
- How sophisticated do the algorithms need to be in order to produce good results?
- There are many issues to resolve from a human factors perspective. Would intelligent analysts and NGOs use such a network?

Conclusion

Bruce.Forrester@drdc-rddc.gc.ca